

Voice over IP Security: Issues and Answers

WHITE PAPER

Sponsored by: General Dynamics

Shawn P. McCarthy
October 2007

INTRODUCTION

Voice over Internet Protocol (VoIP) is an increasingly popular technology that allows participants to make telephone calls using a broadband Internet connection rather than a traditional analog phone line. The solution is sometimes described as Internet telephony, or broadband telephony.

Over the past few years, VoIP has seen significant growth in the commercial sector. Recent IDC reports indicate that roughly 75% of commercial enterprises have some type of VoIP system in use. About 15% use VoIP exclusively.

U.S. federal government offices, which made significant investments in traditional phone lines in the late 1980s and 1990s, have not migrated as quickly to VoIP. Only about 45% of federal government offices have some type of VoIP solution in place. But many are now looking closely at VoIP solutions because of the advanced calling, conferencing, and switching capabilities they can provide and because VoIP often presents a way to quickly reduce telecommunications costs.

This trend is expected to continue, and it's likely that over 70% of federal government offices will have some kind of VoIP solution in place by 2010. Former U.S. Department of Homeland Security (DHS) Secretary Tom Ridge has stated that VoIP won't become a powerful communications tool for security applications until it has penetrated all levels of government. Once it has, VoIP will hold great potential for multiple security applications plus access to multiple stores of data that can quickly be made available to first responders.

Recently, open source VoIP solutions and low-cost hardware have sharply reduced the cost of IP-based PBX ownership.

However, with the VoIP transition, new security issues have arisen. Government offices that are considering a switch to VoIP should carefully consider these issues, along with their potential solutions.

BENEFITS

In a recent survey, about 86% of government VoIP users told IDC that they decided to purchase their VoIP systems because of anticipated cost savings. Multiple aspects should be considered when calculating such a potential return on investment (ROI) for a VoIP system. These may include:

- Lower monthly long distance bills
- Reduced hardware, software, and maintenance costs
- Reduced network management costs
- More efficient line usage
- Increased productivity for both end users and IT staff

The extent of potential savings realized by making an investment in VoIP varies greatly depending on what type of older system is being replaced and what type of current long distance contract an office has in place. Hardware savings can be realized by retiring older high-maintenance PBX equipment or reducing the types of hardware that need to be installed on employee desks. (Many VoIP systems need only a single employee to manage them, and often it takes only part of an employee's time.) Perhaps one of the areas of greatest potential cost savings is system maintenance and management. With an internally maintained VoIP system, the system upgrades or configuration changes can often be done without visiting each phone.

All of these benefits indicate that the growth of VoIP systems in government will continue. But a different, very significant issue also must be addressed: improved security for government VoIP networks.

TRENDS

Government offices have a surprisingly strong preference for managing their voice systems themselves. When IDC surveyed VoIP system owners to see who manages the deployment and day-to-day operations of their IP PBX systems, 71.4% of government offices said they manage their systems in-house, while 28.6% rely on third-party management. In contrast, the national average for all industries was 52.8% for third-party management and 47.2% for in-house management.

Most said they plan to increase their use of VoIP in the years ahead. About 40% reported that they are shopping for systems right now.

SECURITY ISSUES

Very few VoIP solutions offer end-to-end (phone-to-phone) encryption at this time. This is especially troublesome because now several open source solutions facilitate "sniffing" of VoIP conversations. As a result, it is relatively easy to eavesdrop on VoIP calls, and in certain circumstances, a hacker could even change the content of a call.

Some VoIP solutions do offer a minor level of security simply because of their patented audio technology. A proprietary solution can make VoIP calls more difficult to understand and crack. But such "security through obscurity" usually does not serve as a solid long-term strategy.

Government offices, especially defense and national intelligence departments, have a strong need for secure communications. Thus, as promises of system flexibility and cost savings prompt these offices to consider a migration to VoIP, they must also focus on the significant security issues that come with Internet voice systems.

Consider the current climate for older telephone systems. Currently, two major secure telephone devices are approved for classified government communications: the Secure Telephone Unit-Third Generation (STU-III) and the Secure Telephone Equipment (STE) systems. Both rely on technology that is 10 to 20 years old and that was originally designed to operate over analog or Integrated Services Digital Network (ISDN) telecommunications systems. As technology has progressed, these phones have become more costly to maintain and operate because they need extra equipment (compared with today's VoIP solutions), and many of their functions and configuration settings cannot be managed centrally. While both of these devices provided high-assurance secure communications solutions in the past, neither is designed to operate on today's more advanced VoIP networks.

One limited encryption solution is available for classified IP-to-IP calls: voice over secure IP (VoSIP). This can be accomplished by using regular VoIP phones along with inline network encryptors (INEs), which may already be in place on some networks to help secure network data traffic. But this solution ends up severely limiting who can be called. Users can make only secure calls at the security level of the network; they are not able to make nonsecure calls or secure calls to non-IP networks. This essentially closes them off from traditional phone communications.

New applications that address the VoIP security concerns are being developed and offered to the government market. One example is the Sectéra® vIPer™ Phone, developed by General Dynamics C4 Systems.

Sectéra vIPer Phone: A New Certified VoIP Security Solution

The Sectéra vIPer Phone from General Dynamics is a high-assurance secure IP phone; this type of product is just entering the VoIP market. The Sectéra vIPer Phone is designed solely and uniquely for today's advanced IP networks, where it provides end-to-end (phone-to-phone) secure connections. It even can include connections to hundreds of thousands of legacy secure phones via a compatible gateway. The vIPer Phone is a self-contained desktop unit that can both place and receive nonsecure and secure calls, eliminating the need for multiple phones on a single desk.

While the vIPer Phone has all of the features of most commercially available desktop phones, such as a directory, a speakerphone, redial, and a headset connection, it also has a number of features that make it unique. The vIPer Phone allows end users to easily adjust settings as needed for different security levels. In addition, the vIPer Phone has been tested and certified by the National Security Agency (NSA) to protect information that is classified at the top secret (TS) level — even on unprotected IP networks. For end users who do not require Type 1 security, General Dynamics also offers the TalkSECURE™ vIPer, which uses AES encryption to secure communications that are sensitive but unclassified.

Infrastructure Details for the Sectéra vIPer Phone

The vIPer Phone is capable of operating on multiple VoIP networks implemented using the Skinny Call (or Client) Control Protocol (SCCP) developed by Cisco. An enhancement is planned for 3Q08 that will enable the phone to support the Session Initiation Protocol (SIP) standard. Because the vIPer Phone is designed specifically for IP networks, local network or systems administrators will be able to "push" VoIP software upgrades through the network to the vIPer Phone, without end-user or operator involvement. For managers who worry about future compatibility, because the vIPer Phone is software upgradeable, it will be able to evolve with future VoIP capabilities. The vIPer Phone uses only about half of its memory when it ships, leaving 50% available for future upgrades. Most upgrades take less than five minutes.

The vIPer Phone is powered via Power over Ethernet (PoE) supplied by the network. If desired, it also can be powered through a standard 120VAC wall outlet. Support is available for multiple key sets for U.S. government-sponsored interoperability, such as NATO partner or coalition sites.

CONSIDERATIONS

- Whenever a government office is evaluating a new system, including a phone system, it must perform due diligence to ensure that its new solution remains compatible with legacy equipment and that it will be able to make the transition without cutting off workers from communications for a significant length of time.
- While significant cost savings are often achieved by a switch to VoIP, such savings can never be guaranteed. Government agencies should do a detailed cost analysis and calculate what, if any, ROI they might achieve by making the transition.

CONCLUSION

The benefits of VoIP in terms of reduced costs, likely improved efficiencies, and reduced manpower requirements are clear, but achieving secure communications using VoIP has been a significant challenge to date. Government offices that require high-assurance secure communications may want to investigate the Sectéra vIPer Phone as a potential solution to that need. Rather than an add-on, it is an integrated security solution that fits well into a VoIP network. And with NSA Type 1 certification, the Sectéra vIPer Phone is the first Type 1 secure wireline phone specifically designed for VoIP networks.

Because this solution is designed to meet specific government needs, it's likely to be on many agencies' short lists as they consider VoIP equipment for agency desktops.

Copyright Notice

Copyright 2007 Government Insights, an IDC company. Reproduction without written permission is completely forbidden. External Publication of Government Insights Information and Data: Any Government Insights information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate Government Insights Vice President. A draft of the proposed document should accompany any such request. Government Insights reserves the right to deny approval of external usage for any reason.